EUROPÄISCHE
KOMMISSION

Brüssel, den 11.12.2025
COM(2025) 752 final

BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

über die Bewertung der operativen Auswirkungen der Ausübung der in der Verordnung (EU) 2022/991 – insbesondere in Artikel 4 Absatz 1 Buchstabe t, Artikel 18 Absatz 2 Buchstabe e, Artikel 18 Absatz 6a sowie Artikel 18a, Artikel 26, Artikel 26a und Artikel 26b – vorgesehenen Aufgaben gemessen an den Zielen von Europol sowie die Bewertung der Auswirkungen dieser Aufgaben auf die in der Charta der Grundrechte festgelegten Grundrechte und Grundfreiheiten, gemäß Artikel 68 Absatz 3 der Verordnung (EU) 2016/794

{SWD(2025) 404 final}

1. Umfang der Bewertung

Seit der Aufnahme ihrer Tätigkeit im Jahr 1999 hat die **Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) eine zentrale Rolle bei der Bekämpfung der schweren grenzüberschreitenden Kriminalität und des Terrorismus** gespielt und ist zu einer wichtigen Triebkraft für die Zusammenarbeit im Bereich der Strafverfolgung in Europa geworden. Die Sicherheitslandschaft hat sich in den letzten 30 Jahren drastisch gewandelt, und entsprechend hat sich auch die DNA der schweren und organisierten Kriminalität verändert[1]. Für die Mitgliedstaaten sind bei der wirksamen Bekämpfung neu auftretender Bedrohungen neue operative Erfordernisse entstanden, und ihre **Erwartungen an die Unterstützung durch Europol haben sich** ebenfalls **geändert**. Das Mandat von Europol wurde daher mehrfach ersetzt oder geändert, um die Relevanz der Agentur zu erhalten und zu stärken.

Das Mandat von Europol gemäß der Verordnung (EU) 2016/794[2] (im Folgenden „Europol-Verordnung“) wurde zuletzt im Jahr 2022 durch die Verordnung (EU) 2022/991[3] geändert, um neuen Sicherheitsbedrohungen Rechnung zu tragen. Die Europol-Verordnung war in einer neuen Realität, in der Kriminelle die Vorteile des **digitalen Wandels**, **neuer Technologien**, der **Globalisierung** und der **Mobilität** ausnutzen, nicht mehr zweckmäßig[4].

Die **spezifischen Ziele** der Verordnung (EU) 2022/991[5] bestanden in der

- Ermöglichung einer wirksamen Zusammenarbeit zwischen **privaten Parteien** und den Strafverfolgungsbehörden zur Bekämpfung des Missbrauchs grenzüberschreitender Dienste durch Straftäter,
- Befähigung der Strafverfolgungsbehörden zur Analyse **großer und komplexer Datensätze** zur Aufdeckung grenzüberschreitender Verbindungen unter voller Wahrung der **Grundrechte**,
- Befähigung der Mitgliedstaaten, **neue Technologien** für die Strafverfolgung zu nutzen.

Darüber hinaus wurden mit der Verordnung (EU) 2022/991 die für Europol geltenden Datenschutzvorschriften geändert, um ein **hohes Datenschutzniveau** aufrechtzuerhalten und ein Gleichgewicht zwischen den neuen Befugnissen der Agentur zur Verarbeitung personenbezogener Daten und dem Schutz der Privatsphäre und der personenbezogenen Daten der Bürgerinnen und Bürger herzustellen. **Um den Informationsfluss zu erleichtern**, wurden die für Europol geltenden Datenschutzvorschriften weitgehend an diejenigen angeglichen, die für andere Agenturen und Einrichtungen der EU im Bereich Justiz und Inneres (JI) gemäß Kapitel IX der Verordnung (EU) 2018/1725 (im Folgenden „EU-Datenschutzverordnung“ oder „EU-DSVO“) gelten, sowie an die für Strafverfolgungsbehörden der Mitgliedstaaten (im Folgenden „zuständige Behörden“) geltenden Datenschutzvorschriften, die nach ihrem nationalen Recht zur Umsetzung der Richtlinie (EU) 2016/680 (im Folgenden „Richtlinie zum Datenschutz bei der Strafverfolgung“)[6] gelten.

---

1 Europol, „EU Serious and Organised Crime Threat Assessment (SOCTA) – The changing DNA of serious and organised crime“, 2025, online abrufbar unter https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf (EU SOCTA 2025). Siehe auch die Bewertung der Bedrohungslage im Zollbereich (CTA) 2025, online abrufbar unter https://www.douane.gouv.fr/sites/default/files/2025-07/03/Livret-CTA-UE-public_0.pdf.

2 ABl. L 135 vom 24.5.2016, S. 53, ELI: http://data.europa.eu/eli/reg/2016/794/oj.

3 ABl. L 169 vom 27.6.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/991/oj.

4 SWD(2020) 543 final vom 9. Dezember 2020, S. 37, https://eur-lex.europa.eu/resource.html?uri=cellar:1a4d9f40-3b02-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF.

5 Ebenda.

6 ABl. L 119 vom 4.5.2016, S. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj.

Mit der Annahme dieses Berichts kommt die Kommission ihrer Verpflichtung gemäß **Artikel 68 Absatz 3 der Europol-Verordnung** nach, die operativen Auswirkungen der Aufgaben von Europol gemäß der Verordnung (EU) 2022/991 drei Jahre nach ihrem Inkrafttreten zu bewerten[7]. Gemäß dem Auftrag der beiden gesetzgebenden Organe hat die Kommission erstens die **operativen Auswirkungen** einiger der neuen Vorschriften für die Verarbeitung personenbezogener Daten in Bezug auf die Ziele von Europol gemäß Artikel 3 der Europol-Verordnung bewertet (nämlich: Unterstützung und Verstärkung der Tätigkeit der zuständigen Behörden der Mitgliedstaaten und ihrer Zusammenarbeit bei der Verhütung und Bekämpfung von Straftaten, die unter das Mandat von Europol fallen), zweitens die Auswirkungen dieser Vorschriften auf die in der Charta[8] verankerten **Grundrechte und Grundfreiheiten** (im Folgenden „Grundrechte") bewertet und drittens eine **Kosten-Nutzen-Analyse** der damit verbundenen Datenverarbeitungsaufgaben durchgeführt.

Zur Vorbereitung der Überprüfung holten die Kommissionsdienststellen Informationen und Rückmeldungen aus verschiedenen Quellen ein und führten Ad-hoc-Konsultationen mit Europol und den Mitgliedstaaten durch. Die begleitende **Arbeitsunterlage der Kommissionsdienststellen** enthält eine detaillierte Beschreibung des allgemeinen Kontexts und der Methodik der Überprüfung sowie eine umfassende Darstellung der Quellen für Nachweise und Konsultationen, die die wichtigsten in diesem Bericht zusammengefassten Ergebnisse bestätigen.

2. Allgemeiner Kontext

Gemäß Artikel 68 Absatz 3 der Europol-Verordnung befasst sich der vorliegende Bericht der Kommission mit ausgewählten Bestimmungen der Verordnung (EU) 2022/991, wobei der Schwerpunkt auf fünf zentralen Aspekten der Arbeit von Europol liegt.

(1) Externe Dimension: Artikel 4 Absatz 1 Buchstabe t der Europol-Verordnung über Informationsausschreibungen über Staatsangehörige eines Drittstaates im Schengener Informationssystem (SIS) auf Vorschlag von Europol

Angesichts des **globalen Charakters von schwerer Kriminalität und Terrorismus** gewinnen Informationen im Besitz von Drittländern und internationalen Organisationen über Täter und Personen, die solcher Straftaten verdächtigt werden, zunehmend an Bedeutung für die innere Sicherheit der EU. Die externe Dimension der Zusammenarbeit auf dem Gebiet der Strafverfolgung in der EU ist daher für die Mitgliedstaaten ebenso von entscheidender Bedeutung wie die **Rolle von Europol bei der Unterstützung der Mitgliedstaaten in ihren Partnerschaften mit Drittländern** oder Einrichtungen mit Sitz in diesen Ländern. Weitere Anstrengungen werden **in Zukunft unerlässlich** sein, um die globale Sicherheit zu stärken[9].

Mit der Verordnung (EU) 2022/991 wurden bereits wesentliche Änderungen der Europol-Verordnung eingeführt, um die **externe Dimension der Tätigkeiten von Europol** zu stärken, insbesondere durch die Erleichterung des Informationsaustauschs mit Drittstaaten[10] und die

---

7 Diese im Einklang mit Artikel 68 Absatz 3 der Europol-Verordnung durchgeführte Bewertung ist nicht die Bewertung, die gemäß den Leitlinien für eine bessere Rechtsetzung im Hinblick auf einen möglichen Vorschlag für eine Überarbeitung der Europol-Verordnung durchzuführen ist. Siehe auch Abschnitt 4.

8 Charta der Grundrechte der Europäischen Union, ABl. C 326 vom 26.10.2012, S. 391, ELI: http://data.europa.eu/eli/treaty/char_2012/oj.

9 Siehe ProtectEU – eine europäische Strategie für die innere Sicherheit, COM(2025) 148 final vom 1. April 2025, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52025DC0148.

10 Siehe beispielsweise Artikel 25 Absatz 4a der Europol-Verordnung, der die Möglichkeit für Europol vorsieht, Daten an Drittstaaten zu übermitteln, wenn Europol alle Umstände der Übermittlung personenbezogener Daten selbst beurteilt hat und zu der Auffassung gelangt ist, dass geeignete Garantien

Verpflichtung von Europol, eine Strategie für die Beziehungen zu Drittstaaten und internationalen Organisationen in ihre mehrjährige Programmplanung und das jährliche Arbeitsprogramm aufzunehmen[11].

Mit **Artikel 4 Absatz 1 Buchstabe t der Europol-Verordnung** wurde Europol eine neue Aufgabe übertragen: Unterstützung der Mitgliedstaaten bei der Verarbeitung von Daten, die von Drittstaaten oder internationalen Organisationen übermittelt werden und an Terrorismus oder schwerer Kriminalität beteiligte Personen betreffen. Dazu gehört auch der **Vorschlag der möglichen Eingabe von Informationsausschreibungen über Staatsangehörige eines Drittstaates im Interesse der Union in das Schengener Informationssystem (SIS) durch die Mitgliedstaaten**. Diese neue Kategorie von Informationsausschreibungen wurde im Jahr 2022[12] infolge einer Änderung der Verordnung (EU) 2018/1862 über die Nutzung des SIS im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen[13] eingeführt.

Bestimmte Informationen, insbesondere wenn es sich bei der betroffenen Person nicht um einen EU-Bürger handelt und keine Verbindung zu einem nationalen Fall besteht, werden von dem Drittstaat nur an Europol weitergegeben, die die Daten verarbeitet und ihre Analyseergebnisse an alle Mitgliedstaaten weitergibt. Ziel der neuen Bestimmungen war es, **die Nutzung von Informationen**, die Europol von Drittstaaten erhält, **zu maximieren**, indem sie leichter zugänglich gemacht werden, als wenn sie nur über das Europol-eigene System verfügbar wären. Es ergänzte andere Maßnahmen wie das Europäische Suchportal (European Search Portal, im Folgenden „ESP“) und den Interoperabilitätsrahmen[14] zwischen EU-Informationssystemen für Sicherheit, Grenzmanagement und Migrationssteuerung, um die strukturellen Mängel im Zusammenhang mit diesen Systemen zu beheben, die die Arbeit der nationalen Behörden und insbesondere der Grenzschutzbeamten behindern.

Das **SIS** wird als ein **wichtiger zusätzlicher Verbreitungskanal** angesehen: Es ist die am häufigsten verwendete Datenbank für Strafverfolgung, Grenzkontrollen und Migration in Europa. Im Jahr 2024 wurden mehr als 15 Milliarden Abfragen im SIS durchgeführt, gegenüber etwa 14 Millionen Abfragen im Europol-Informationssystem (EIS) und weniger als 3 Milliarden Abfragen (weltweit) in den 19 Interpol-Datenbanken, den beiden anderen führenden Informationssystemen für die zuständigen Behörden[15].

---

für den Schutz dieser Daten bestehen, und Artikel 25 Absatz 5 der Europol-Verordnung, in dem der Anwendungsbereich der Ausnahmefälle, in denen Europol in hinreichend begründeten Fällen (Kategorien von) Daten ad-hoc an Drittstaaten und internationale Organisationen übermitteln kann, ausgeweitet wird.

11 Artikel 12 Absatz 2 der Europol-Verordnung.

12 Verordnung (EU) 2022/1190; ABl. L 185 vom 12.7.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/1190/oj.

13 Verordnung (EU) 2018/1862; ABl. L 312 vom 7.12.2018, S. 56, ELI: http://data.europa.eu/eli/reg/2018/1862/oj.

14 Verordnung (EU) 2019/818; ABl. L 135 vom 22.5.2019, S. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

15 eu-LISA 2024 SIS Annual Report, online abrufbar unter https://www.eulisa.europa.eu/sites/default/files/documents/sis-annual-report-2024.pdf, Europol, Consolidated Annual Activity Report (CAAR) 2024, online abrufbar unter https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated_Annual_Activity_Report_2024.PDF und https://www.interpol.int/How-we-work/Databases.

(2) <u>Innovation</u>: Artikel 18 Absatz 2 Buchstabe e und Artikel 33a der Europol-Verordnung über die Verarbeitung personenbezogener Daten durch Europol für Innovations- und Forschungsprojekte

Die technologischen Entwicklungen bergen sowohl enorme Chancen als auch beträchtliche Herausforderungen für die innere Sicherheit der EU[16] und haben sich so tiefgreifend auf die Kriminalität ausgewirkt, dass sich sogar die „DNA" der Bedrohungen durch schwere und organisierte Kriminalität[17] verändert hat. Kriminelle integrieren neue Technologien rasch in ihre Aktivitäten, entwickeln neue Geschäftsmodelle und verfeinern ihre Taktiken. Gleichzeitig bieten diese Fortschritte **den Strafverfolgungsbehörden beispiellose Möglichkeiten, ihre Fähigkeiten auszubauen**. Daher spielen Forschung und Innovation eine entscheidende Rolle für die innere Sicherheit, indem sie Lösungen entwickeln, um neuen Bedrohungen entgegenzuwirken und mit den sich rasch entwickelnden Formen und Vorgehensweisen krimineller Netze, einschließlich solcher, die sich aus dem Missbrauch von Technologie ergeben, Schritt zu halten. Die Union hat im Rahmen von **ProtectEU**, der Europäischen Strategie für die innere Sicherheit[18], in die Entwicklung innovativer Instrumente durch EU-finanzierte sicherheitsbezogene Forschung und Innovation investiert und wird dies auch weiterhin tun.

Das **Europol-Innovationslabor (EIL)**[19], das Ende 2019 im Auftrag der JI-Minister der EU-Mitgliedstaaten eingerichtet wurde, soll das Engagement von Europol für Innovationen im Bereich der Strafverfolgung vorantreiben. Mit der Verordnung (EU) 2022/991 wurden wesentliche Änderungen der Europol-Verordnung eingeführt, um das Mandat von Europol für Innovation zu stärken, um sowohl das Potenzial des EIL als auch Synergien mit anderen Forschungs- und Innovationstätigkeiten auf EU-Ebene, insbesondere in der Kommission, im Rahmen des **EU-Innovationszentrums** für die innere Sicherheit[20] zu fördern.

Artikel 18 Absatz 2 der Europol-Verordnung über die Zwecke der Informationsverarbeitung wurde geändert, um Europol die **Verarbeitung operativer personenbezogener Daten** auch **für Forschungs- und Innovationsprojekte** zu ermöglichen. Die Verfügbarkeit hochwertiger Datensätze, die eine empirische Prüfung der Validität neuer Instrumente ermöglichen, wird allgemein als wichtige Voraussetzung für die Entwicklung von Technologien angesehen. Im Gegensatz dazu können unzuverlässige oder verzerrte Datensätze für Tests dazu führen, dass schlechte Technologien hergestellt werden[21].

In Artikel 18 Absatz 3a, Artikel 30 Absätze 2 und 3 sowie **Artikel 33a der Europol-Verordnung** wurden maßgeschneiderte Datenschutzgarantien für eine solche Verarbeitung festgelegt. Der letztgenannte Artikel sah die Einrichtung einer **Reallabor-Umgebung** vor, indem festgelegt wurde, dass personenbezogene Daten, die im Rahmen eines Projekts verarbeitet werden, vorübergehend in eine getrennte, isolierte und geschützte Datenverarbeitungsumgebung innerhalb von Europol ausschließlich zur Durchführung des betreffenden Projekts kopiert werden.

---

16 Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024, online abrufbar unter Internet Organised Crime Threat Assessment (IOCTA) 2024, Europol.

17 Europol, EU SOCTA 2025, S. 19.

18 COM(2025) 148 final vom 1. April 2025, S. 9, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52025DC0148.

19 https://www.europol.europa.eu/how-we-work/innovation-lab.

20 Vgl. insbesondere Artikel 4 Absatz 1 Buchstaben v und w der Europol-Verordnung.

21 SWD(2020) 543 final vom 9. Dezember 2020, S. 29.

(3) <u>Strafrechtliche Ermittlungen</u>: Artikel 18 Absatz 6a und Artikel 18a der Europol-Verordnung über die Bedingungen für die Verarbeitung personenbezogener Daten, die ohne die Kategorisierung betroffener Personen (Data Subject Categorisation, DSC) eingegangen sind

In ihrer Rolle als **EU-Sammelstelle für kriminalpolizeiliche Informationen** erleichtert Europol nicht nur die Erhebung und den Austausch von Informationen, sondern trägt auch dazu bei, **die Wirksamkeit von Ermittlungen durch fortgeschrittene Datenanalysen** und die Aufdeckung grenzüberschreitender Verbindungen zwischen Straftaten und kriminellen Netzen, die auf nationaler Ebene nicht sichtbar sind, **zu erhöhen**. Diese Fähigkeiten unterstützen die Mitgliedstaaten, indem sie die für ihre strafrechtlichen Ermittlungen verfügbaren Informationen erweitern.

Durch den umfassenden und intensiven Einsatz von Technologie **sind große und komplexe Datensätze in allen Lebensbereichen**, einschließlich der Kriminalität, **zur neuen Normalität geworden**[22]. Im Rahmen von Ermittlungen im Bereich der organisierten Kriminalität oder des Terrorismus besteht zunehmend die Herausforderung, große Mengen elektronisch gespeicherter Daten zu analysieren, die oft Terabytes umfassen, darunter auch Audio- und Videodaten sowie maschinell erzeugte Daten, die bei Ermittlungen beschlagnahmt wurden. So analysierten die Ermittler im Rahmen der gemeinsamen Ermittlungen zur Zerschlagung des EncroChat-Netzwerks[23] Millionen von Nachrichten, die Kriminelle zur Planung schwerer Straftaten ausgetauscht haben. Vor diesem Hintergrund ist es für die Strafverfolgungs- und Justizbehörden von entscheidender Bedeutung, dass sie über die notwendigen Instrumente, Fachkenntnisse und Ressourcen der Informations- und Kommunikationstechnologie (IKT) verfügen, um große und komplexe Datensätze (im Fachjargon als „Big Data“[24] bezeichnet) zu analysieren.

Zwar enthielt die im Jahr 2016 angenommene Europol-Verordnung keine Beschränkungen für die Analyse von Big Data an sich, es fehlten jedoch strukturierte Bestimmungen, in denen die Bedingungen für die Analyse dieser Art von Daten festgelegt sind. Der **kritischste Punkt** war die **Anforderung der Kategorisierung betroffener Personen**. Der Begriff „Kategorisierung betroffener Personen“ bezieht sich auf die Notwendigkeit, die Datensätze zu überprüfen, um personenbezogene Daten nach verschiedenen, in Anhang II.A und Anhang II.B der Europol-Verordnung erschöpfend aufgeführten Kategorien zu sortieren, bevor die Daten zu Ermittlungszwecken tatsächlich verarbeitet werden, auch vor dem Abgleich von Daten, um Verbindungen aufzudecken oder strategische oder thematische Analysen oder operative Analysen durchzuführen[25]. Die einschlägigen Kategorien sind mit verschiedenen Arten der Beteiligung an strafrechtlichen Ermittlungen verknüpft, darunter i) Verdächtige, potenzielle künftige Straftäter sowie ii) Kontakte, Verbündete, Opfer, Zeugen und Informanten im Zusammenhang mit kriminellen Tätigkeiten. Im Allgemeinen darf Europol die

---

22 Europol, EU SOCTA 2025, passim.

23 https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized.

24 EDSB, Stellungnahme 7/2015, S. 7, abrufbar unter https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_de.pdf. „Allgemein ausgedrückt bezieht sich der Begriff ‚**Big Data**‘ als gemeinsamer Nenner unterschiedlicher Definitionen auf die Praxis des Kombinierens immenser Mengen von Informationen aus verschiedenen Quellen und ihre Analyse; dabei kommen komplexere Algorithmen als Grundlage der Entscheidungsfindung zur Anwendung. Big Data beruht nicht nur auf der zunehmenden Fähigkeit der Technologie, die Erhebung und Speicherung großer Datenmengen zu unterstützen, sondern auch auf ihrer Fähigkeit, den vollständigen Wert von Daten zu analysieren, zu verstehen und zu nutzen (insbesondere anhand von Analyseanwendungen).“

25 Siehe Artikel 18 Absatz 2 der Europol-Verordnung.

personenbezogenen Daten von Personen, die unter keine dieser Kategorien fallen, weder verarbeiten noch speichern.

Datenlieferanten wie **Mitgliedstaaten** oder **Einrichtungen und Agenturen der EU** führen **in der Regel** bereits die Kategorisierung betroffener Personen durch, bevor sie die personenbezogenen Daten an Europol übermitteln[26]. Nach EU-Recht sind sie alle verpflichtet, die Kategorisierung betroffener Personen für ihre eigenen Verarbeitungen und Ermittlungen durchzuführen, unabhängig von der Datenübermittlung an Europol und auf der Grundlage gleichwertiger, aber nicht identischer Vorschriften wie Europol[27]. Bei großen und komplexen Datensätzen ist die manuelle Vorverarbeitung jedoch eine ressourcen- und zeitaufwendige Aufgabe. Die Analyse der Daten eines einzigen Mobiltelefons kann halbautomatisch bis zu drei Tage dauern, und bei einer Untersuchung können sogar Hunderte von Mobiltelefonen beschlagnahmt werden. Die Kategorisierung betroffener Personen **im Bereich Big Data** ist aufgrund des schieren Umfangs der Datensätze, der Art und Weise, wie die Daten (un-)strukturiert sind, des Mangels an Ressourcen oder des hohen **manuellen Aufwands nicht immer möglich**. In der Praxis besteht die einzige Möglichkeit darin, die Daten zunächst aus operativer Sicht eingehender zu analysieren oder Verbindungen – auch halbautomatisch – durch einen Abgleich der verfügbaren Daten aufzudecken.

In der Verordnung (EU) 2022/991 wurden die Bedingungen für die Kategorisierung betroffener Personen präzisiert, um **Rechtssicherheit** in Bezug auf die Verarbeitung großer und komplexer Datensätze zu schaffen. Europol und der Europäische Datenschutzbeauftragte (EDSB) haben den Wortlaut und den Geist der Europol-Verordnung in Bezug auf die geltende Datenspeicherfrist unterschiedlich ausgelegt. Laut Europol sollte dieser Zeitraum drei Jahre betragen; nach Ansicht des EDSB sollte die Frist sechs Monate betragen[28]. Außerdem waren neue Bestimmungen erforderlich, um für **mehr Flexibilität** zu sorgen und ein angemessenes Gleichgewicht zwischen Datenschutz und Sicherheitsaspekten herzustellen.

In Artikel 18 Absatz 5a der Europol-Verordnung in Verbindung mit Artikel 73 der EU-DSVO wurde zunächst der allgemeine Grundsatz der Kategorisierung betroffener Personen gemäß Artikel 18 Absatz 2 und Anhang II präzisiert. Europol hat die Aufgabe, gegebenenfalls und so weit wie möglich eine **eindeutige Zuordnung von personenbezogenen Daten zu einer bestimmten Kategorie von betroffenen Personen** vorzunehmen. In der Praxis sollte Europol in der Regel die genaue Rolle bei der kriminellen Aktivität (z. B. ob es sich bei einer Person um einen Verdächtigen, ein Opfer oder nur um einen Zeugen handelt) für jede Person festlegen, deren personenbezogene Daten verarbeitet werden, und nicht auf aggregierter Ebene für alle Personen in einer zu verarbeitenden Datei oder einem Teil davon (z. B. indem sie einfach feststellt, dass alle genannten Personen an einer kriminellen Tätigkeit beteiligt sind, die unter ihr Mandat fällt, und zwar auf der Grundlage einer Prüfung der allgemeinen Umstände, die zu der Datei geführt haben), bevor personenbezogene Daten verarbeitet werden können.

Artikel 18 Absatz 6a der Europol-Verordnung gestattet ausdrücklich die Verarbeitung personenbezogener Daten, die ohne Kategorisierung betroffener Personen eingegangen sind,

---

26 Die Mitgliedstaaten übermitteln Europol Daten über ihre Netzanwendung für sicheren Datenaustausch (SIENA), in der die Kategorisierung betroffener Personen als Pflichtfeld implementiert wird.

27 Siehe beispielsweise Artikel 6 der Richtlinie (EU) 2016/680 (im Folgenden „Richtlinie zum Datenschutz bei der Strafverfolgung“ in Bezug auf indirekt zuständige Behörden); ABl. L 119 vom 4.5.2016, S. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj; Artikel 51 der Verordnung (EU) 2017/1939 des Rates (im Folgenden „EUStA-Verordnung“); ABl. L 283 vom 31.10.2017, S. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj; Artikel 27 Absatz 3 der Verordnung (EU) 2018/1727 (im Folgenden „Eurojust-Verordnung“); ABl. L 295 vom 21.11.2018, S. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj.

28 https://www.edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf.

für einen Zeitraum von **bis zu 18 Monaten**, der in begründeten Fällen auf bis zu 36 Monate verlängert werden kann, und zwar ausschließlich **zum Zwecke der Vervollständigung der Kategorisierung betroffener Personen**. Artikel 18 Absatz 6a der Europol-Verordnung bezieht sich nicht ausdrücklich auf große und komplexe Datensätze, sondern sieht allgemein die Prüfung vor, ob die Verarbeitung „**unbedingt erforderlich**" ist.

Artikel 18a der Europol-Verordnung sieht eine Ausnahmeregelung vor, wonach Europol personenbezogene Daten, die sie von einer **zuständigen Behörde**, der Europäischen Staatsanwaltschaft (**EUStA**) oder **Eurojust** erhalten hat, verarbeiten kann, wenn dies zur Unterstützung **laufender strafrechtlicher Ermittlungen** erforderlich ist, ohne dass eine Kategorisierung betroffener Personen durchgeführt werden muss, sofern dies noch nicht erfolgt ist, und die über die in der Europol-Verordnung aufgeführten Kategorien betroffener Personen hinausgehen. Europol kann die Daten durch **operative Analysen** oder in hinreichend begründeten Ausnahmefällen durch einen **Abgleich** zur Ermittlung etwaiger Zusammenhänge oder anderer relevanter Verbindungen verarbeiten. Mit dieser Ausnahmeregelung sollte den Unterschieden zwischen den für Europol geltenden Vorschriften über die Kategorisierung betroffener Personen und den für die zuständigen Behörden, die EUStA und Eurojust geltenden Vorschriften Rechnung getragen werden.

(4) Zusammenarbeit mit Dritten: Artikel 26, 26a und 26b der Europol-Verordnung über den Austausch personenbezogener Daten zwischen Europol und privaten Parteien

Kriminelle missbrauchen zunehmend die (grenzüberschreitenden) Dienstleistungen privater Parteien – internetgestützte, finanzielle und klassische Telekommunikationsdienste. Folglich **verfügen private Parteien über eine große Menge personenbezogener Daten, die für strafrechtliche Ermittlungen relevant sind**. Insbesondere hat das Internet einen öffentlichen Raum geschaffen, der sich faktisch in privater Hand befindet, was es schwierig macht, Regeln online zu Strafverfolgungszwecken ebenso wirksam durchzusetzen wie offline[29].

Vor diesem Hintergrund ist die **Zusammenarbeit zwischen Strafverfolgungsbehörden und privaten Parteien unverzichtbar** geworden. Wie in **ProtectEU**, der Europäischen Strategie für die innere Sicherheit, dargelegt, wird es von entscheidender Bedeutung sein, die Partnerschaften mit dem Privatsektor zu intensivieren, um den Informationsaustausch zu erleichtern[30]. Die Polizeichefs haben in ihrer gemeinsamen Erklärung zur Zukunft von Europol[31] auch gefordert, Europol solle als **zentrales Zugangstor für die Einholung von Informationen von privaten Einrichtungen** dienen. Diese Zusammenarbeit reicht vom Austausch von Informationen und der Bereitstellung kommerzieller Daten aus allgemein zugänglichen Quellen bis hin zur Beteiligung an Forschungs- und Innovationsprojekten und zur Erbringung von Dienstleistungen, die das Funktionieren der Unternehmen unterstützen[32]. So hat Europol beispielsweise im Jahr 2025 erfolgreich Lumma-Stealer, die weltweit größte Bedrohung durch Infostealer, durch die Zusammenarbeit mit Microsoft, das mehr als

---

29 SWD(2020) 543 final vom 9. Dezember 2020, S. 16.

30 Siehe ProtectEU – eine Europäische Strategie für die innere Sicherheit, S. 6.

31 https://prezydencja.policja.pl/ppl/aktualnosci/260402,Wspolna-Deklaracja-Europejskich-Szefow-Policji-w-sprawie-przyszlosci-Europolu-Jo.html.

32 Europol, Cooperation with Private Parties, 31. Mai 2023, EDOC #1306090v13. Siehe auch Milieu Consulting, Study on the Practice of direct exchange with of personal data between Europol and Private Parties, Final Report, September 2020.

394 000 Windows-Computer ermittelt hatte, die weltweit mit der Lumma-Malware infiziert waren, zerstört[33].

Mit der Verordnung (EU) 2022/991 wurden **zusätzliche Möglichkeiten** für Europol eingeführt, personenbezogene Daten mit privaten Parteien auszutauschen. Bisher konnte Europol personenbezogene Daten von privaten Parteien nur über eine nationale Europol-Stelle oder über vorab ermittelte Kontaktstellen oder Behörden von Drittstaaten oder internationalen Organisationen erhalten. Der Zweck der Verarbeitung durch Europol beschränkte sich auf die Ermittlung der zuständigen nationalen Europol-Stelle oder der Kontaktstelle oder Behörde des Drittstaats und der internationalen Organisation, die die Zuständigkeit für den Fall übernehmen könnte.

Mit dem geänderten Artikel 26 der Europol-Verordnung wurde die Aufgabe von Europol erweitert, sodass Europol die Informationen (einschließlich personenbezogener Daten) von privaten Parteien umfassend verarbeiten kann. Ein Hauptzweck der Verarbeitung besteht nach wie vor darin, die betreffende nationale Europol-Stelle zu identifizieren. Europol ist jedoch nunmehr auch befugt, die Informationen durch eine eigene Analyse zu ergänzen, um die weitere Bearbeitung eines Falls auf nationaler Ebene zu erleichtern.

Zusätzlich zu den horizontalen Bestimmungen des Artikels 26 der Europol-Verordnung wurden mit Artikel 26a Vorschriften für **Online-Krisensituationen** eingeführt, und Artikel 26b befasste sich mit der **Verbreitung von Darstellungen sexuellen Missbrauchs von Kindern im Internet**. In diesen Fällen kann Europol die Mitgliedstaaten durch die Verarbeitung personenbezogener Daten, die sie direkt von privaten Parteien erhalten hat, unterstützen. Europol kann auch im Einzelfall personenbezogene Daten an private Parteien übermitteln.

Mit der Verordnung (EU) 2022/991 wurde die Möglichkeit eingeführt, die Infrastruktur von Europol für den Informationsaustausch zwischen zuständigen Behörden und privaten Parteien zu nutzen, sowie die Möglichkeit für Europol, die Mitgliedstaaten zu ersuchen, gemäß deren nationalen Rechtsvorschriften personenbezogene Daten von privaten Parteien zu erlangen.

Diese Bestimmungen wurden im Einklang mit anderen Initiativen wie der Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte[34] und dem Gesetz über digitale Dienste[35] angenommen. Weitere Maßnahmen zur stärkeren Beteiligung privater Parteien an der Kriminalitätsbekämpfung und zur Erleichterung des rechtmäßigen Zugangs zu Daten sind geplant, um im Rahmen von **ProtectEU**, der Europäischen Strategie für die innere Sicherheit, das Ziel einer „Veränderung der Sicherheitskultur“ zu verwirklichen (**gesamtgesellschaftlicher Ansatz**)[36].

(5) Interne und externe Aufsicht über die Achtung der Grundrechte durch Europol

In der Verordnung (EU) 2022/991 wird die Verpflichtung von Europol betont, die Grundrechte gemäß den Bestimmungen zu achten, in denen die Aufgaben von Europol und verbesserte damit verbundene Garantien festgelegt sind, insbesondere durch eine **Stärkung der internen und externen Aufsicht über die Agentur**.

---

33 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world's-largest-infostealer-lumma. Weitere Beispiele sind der begleitenden Arbeitsunterlage der Kommissionsdienststellen zu entnehmen.

34 Verordnung (EU) 2021/784; ABl. L 172 vom 17.5.2021, S. 79, ELI: http://data.europa.eu/eli/reg/2021/784/oj.

35 Verordnung (EU) 2022/2065; ABl. L 277 vom 27.10.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

36 Siehe ProtectEU – eine Europäische Strategie für die innere Sicherheit, S. 2.

Im Bereich des Datenschutzes bedeutete die Angleichung der Europol-Verordnung an die Datenschutzgarantien im Rahmen der EU-DSVO die Einführung neuer Vorschriften für die Aufsicht durch den **Datenschutzbeauftragten** (DSB) und den **Europäischen Datenschutzbeauftragten** (EDSB). So ist beispielsweise die Verpflichtung zur Vorlage einer Datenschutz-Folgenabschätzung und der vorherigen Konsultation des EDSB für jede neue Art der Verarbeitung systematisch geworden. Mit der Verordnung (EU) 2022/991 wurde auch eine neue Zuständigkeit von Europol für Anträge auf Zugangsrechte eingeführt. Zuvor waren die zuständigen nationalen Behörden für die Bearbeitung von Anträgen auf Zugangsrechte zuständig, wenn die Mitgliedstaaten die Datenlieferanten waren.

Mit der Verordnung (EU) 2022/991 wurde auch ein **neuer Posten des Grundrechtsbeauftragten** bei Europol eingeführt, der unter anderem damit betraut ist, den Exekutivdirektor von Europol über mögliche Verstöße gegen die Grundrechte im Zuge der Tätigkeiten der Agentur zu informieren.

Darüber hinaus wurden die **demokratische Kontrolle und Rechenschaftspflicht** durch die politische Überwachung der Tätigkeiten von Europol durch das **Europäische Parlament und die nationalen Parlamente** gemäß Artikel 88 Absatz 2 Unterabsatz 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) **gestärkt**. Mit der Verordnung (EU) 2022/991 wurde die Überwachung durch den **Gemeinsamen parlamentarischen Kontrollausschuss**[37] gestärkt. So sah sie beispielsweise die obligatorische Anhörung des Gemeinsamen parlamentarischen Kontrollausschusses zum Entwurf der mehrjährigen Programmplanung und des jährlichen Arbeitsprogramms von Europol, die Möglichkeit für den Gemeinsamen parlamentarischen Kontrollausschuss, unverbindliche konkrete Empfehlungen an Europol zu richten und sie dem Europäischen Parlament und den nationalen Parlamenten vorzulegen, sowie die Einsetzung eines Konsultationsforums, das den Gemeinsamen parlamentarischen Kontrollausschuss auf Anfrage unterstützt, indem es unabhängige Beratung in Grundrechtsfragen leistet, vor.

3. Wichtigste Ergebnisse der Bewertung

3.1. Stand der operativen Umsetzung der neuen Befugnisse und Aufgaben von Europol im Bereich der Verarbeitung personenbezogener Daten

Die Verordnung (EU) 2022/991 trat **am 28. Juni 2022 in Kraft**. Ihre operative Umsetzung hing jedoch von verschiedenen Governance-, technischen und administrativen Maßnahmen sowie operativen Anforderungen ab, z. B. in einigen Fällen von der Einrichtung neuer IKT-Strukturen.

Drei Jahre später **sind fast alle** in Artikel 68 Absatz 3 der Verordnung (EU) 2022/991 aufgeführten **Bestimmungen in Kraft getreten**. Die Bestimmungen über die Analyse großer und komplexer Datensätze (Artikel 18 Absatz 6a und Artikel 18a der Europol-Verordnung) und die Zusammenarbeit mit privaten Parteien (Artikel 26, 26a und 26b der Europol-Verordnung) galten ab dem 28. Juni 2022 oder kurz danach. Die Verarbeitung personenbezogener Daten für Forschungs- und Innovationsprojekte (Artikel 18 Absatz 2 Buchstabe e der Europol-Verordnung) begann im Jahr 2023, nachdem die Reallabor-Umgebung namens ODIN eingerichtet wurde, um die spezifischen Datenschutzanforderungen nach Artikel 33a der Europol-Verordnung zu erfüllen. Am 29. Juni 2025 war die Möglichkeit für Europol, **Informationsausschreibungen im SIS** durch die Mitgliedstaaten gemäß Artikel 4 Absatz 1 Buchstabe t der Europol-Verordnung vorzuschlagen, noch nicht

[37] Siehe https://www.europarl.europa.eu/relnatparl/en/eu-agencies-oversight/jpsg-on-europol.

einsatzbereit, da die technische Umsetzung der neuen Ausschreibungsart noch nicht abgeschlossen ist. Die Inbetriebnahme **erfolgt voraussichtlich im Jahr 2026**.

3.2. Bewertung der operativen Auswirkungen der neuen Befugnisse und Aufgaben von Europol im Bereich der Verarbeitung personenbezogener Daten auf die Ziele der Agentur gemäß Artikel 3 der Europol-Verordnung

Was die operativen Auswirkungen der neuen Befugnisse und Aufgaben von Europol im Bereich der Verarbeitung personenbezogener Daten betrifft, so ergab die Konsultation, dass **die Mitgliedstaaten insgesamt ein positives Bild** von deren Relevanz, Wirksamkeit und Mehrwert sowie von der Unterstützung ihrer zuständigen Behörden in den damit verbundenen Bereichen durch Europol **haben**[38].

Die Untersuchungsbefugnisse, die Gegenstand dieser Bewertung sind, werden nicht kontinuierlich oder systematisch genutzt, um Daten zu Überwachungszwecken zu verarbeiten; bei einigen handelt es sich sogar um Ausnahmefälle, während andere regelmäßig und bedarfsorientiert bei Untersuchungen eingesetzt werden. Die **operative Anwendung der neuen Bestimmungen** während des Berichtszeitraums **war quantitativ sehr unterschiedlich**, je nach den verschiedenen technischen Merkmalen und rechtlichen Bedingungen, die mit den neuen Bestimmungen verbunden sind.

Europol erhielt von den Mitgliedstaaten eine **nicht unerhebliche** Zahl **neuer Beiträge ohne Kategorisierung betroffener Personen** gemäß Artikel 18 Absatz 6a der Europol-Verordnung, die sich im Jahr 2023 auf 653 und 2024 auf 597 beliefen. Es gab keinen kurzfristigen Anstieg der Beiträge ohne Kategorisierung betroffener Personen, und die Zahl der Fälle, in denen Artikel 18 Absatz 6a angewandt wurde, blieb im Vergleich zu gleichwertigen Fällen im Zeitraum vor dem 28. Juni 2022 **konstant**. Die neuen Bestimmungen hatten auch keine negativen Auswirkungen auf das Engagement der Mitgliedstaaten bei der Durchführung der Kategorisierung betroffener Personen[39]. Zwischen 2023 und 2024 machte der Anteil der Beiträge ohne Kategorisierung betroffener Personen **weniger als 1 % aller** von Europol akzeptierten **Beiträge** der Mitgliedstaaten aus (0,85 % im Jahr 2023 und 0,71 % im Jahr 2024). Seit Juni 2022 hat Europol die Kategorisierung betroffener Personen innerhalb von 18 Monaten kontinuierlich abgeschlossen, ohne die verlängerte Frist von 36 Monaten in Anspruch zu nehmen. Europol und sechs Mitgliedstaaten betonten, dass trotz der verbesserten Rechtssicherheit der **Verwaltungsaufwand** sowohl für Europol als auch für die zuständigen Behörden aufgrund der Anstrengungen, die erforderlich sind, um der Kategorisierung personenbezogener Daten durch individuelle Beteiligung an der Straftat nachzukommen, **weiterhin erheblich** ist. Diese Anforderung wird von Europol sehr streng umgesetzt[40].

Europol berichtete, dass der Informationsaustausch mit **privaten Parteien** im Jahr 2023 nach wie vor vernachlässigbar war, da nur 26 Fälle der Umsetzung von Artikel 26 der Europol-Verordnung verzeichnet wurden (zusätzlich zu den Fällen, die unter das Gesetz über digitale Dienste fallen)[41]. Im Jahr **2024** zeigten die Statistiken jedoch einen **starken Anstieg auf**

---

38 Siehe die in Abschnitt 5 der diesen Bericht begleitenden Arbeitsunterlage der Kommissionsdienststellen vorgelegten Nachweise, insbesondere die Beiträge von Europol und die Antworten der Mitgliedstaaten auf die Fragen 2, 4 und 5 des kurzen Fragebogens vom 2. Juni 2025 in Anhang III der Arbeitsunterlage der Kommissionsdienststellen.

39 Wie ein Mitgliedstaat während der Konsultation hervorgehoben hat, können „[d]ie Mitgliedstaaten ... klar unterscheiden, mit welcher Art von Daten [sie] zu tun haben, was für die Untersuchung selbst von großer Bedeutung sein kann“.

40 Siehe Unterabschnitt 7.1.3 der diesen Bericht begleitenden Arbeitsunterlage der Kommissionsdienststellen und die Antworten der Mitgliedstaaten auf Frage 9 des kurzen Fragebogens vom 2. Juni 2025 in Anhang III der Arbeitsunterlage der Kommissionsdienststellen.

41 Europol, Bericht 2023 gemäß Artikel 16 Absatz 11 der Europol-Verordnung.

284 Fälle (fast + 1 000 %) im Zusammenhang mit der Zusammenarbeit mit privaten Parteien nach Artikel 26 der Europol-Verordnung. Dies gilt insbesondere für Daten privater Unternehmen zur Ermittlung von **Finanz- und Wirtschaftskriminalität**. Europol hat Artikel 26b der Europol-Verordnung auch bei der Bekämpfung der sexuellen Ausbeutung von Kindern in erheblichem Umfang genutzt, wo die Zusammenarbeit mit privaten Parteien bereits zuvor sehr umfangreich war. In beiden Fällen umfassen die Daten auch die Zusammenarbeit, die nach dem vorherigen Rechtsrahmen möglich war. Aus den verfügbaren Daten geht nicht hervor, inwieweit diese neuen Fälle unter die neuen Bestimmungen oder eine verstärkte Nutzung bestehender Möglichkeiten fallen.

Im Jahr **2025** hat Europol eine **neue Strategie** zur weiteren Verbesserung der Zusammenarbeit mit privaten Parteien angenommen. Darüber hinaus wurden Maßnahmen ergriffen, um die IKT-Infrastruktur von Europol, die den zuständigen Behörden für den Informationsaustausch mit privaten Parteien zur Verfügung steht, zu verbessern. Im Jahr **2023** startete Europol die „Plateforme Européenne de Retraits de Contenus illégaux sur Internet“ (**PERCI**), um die Umsetzung der Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte und in Zukunft möglicherweise auch des Artikels 18 des Gesetzes über digitale Dienste sowie des Meldedienstes der EU für Kindesmissbrauch (**EU CARES**) zu erleichtern. PERCI ist nicht in das Europol-Informationssystem (EIS) integriert[42].

Andere Bestimmungen wurden überhaupt **nicht angewandt** (Artikel 26a der Europol-Verordnung), obwohl sie betriebsbereit waren, **oder** wurden **nur ausnahmsweise** angewandt (ein Fall, in dem Artikel 18a der Europol-Verordnung im Jahr 2024 angewandt wurde, und ein Projekt, das mit der Verarbeitung personenbezogener Daten gemäß Artikel 18 Absatz 1 Buchstabe t der Europol-Verordnung im Jahr 2025 durchgeführt wurde, wobei drei neue Projekte bereits in Vorbereitung waren).

Aufgrund des begrenzten Zeitraums der operativen Umsetzung der mit der Verordnung (EU) 2022/991 eingeführten Bestimmungen und der langwierigen strafrechtlichen Ermittlungen und Gerichtsverfahren waren die Mitgliedstaaten nicht in der Lage, quantitative Daten zu den operativen Auswirkungen dieser Bestimmungen vorzulegen. Stattdessen boten sie einige Beispiele für erfolgreiche Ermittlungen an, die den **greifbaren Nutzen der neuen Ermittlungsmöglichkeiten in realen Situationen** für die bereits geltenden Bestimmungen belegen, wie z. B. EncroChat, Sky ECC, auf dem Balkan ansässige kriminelle Netze, die am Kokainhandel beteiligt sind, oder Lumma-Stealer.

Europol und acht Mitgliedstaaten wiesen auch auf einige **verbesserungsbedürftige Bereiche** hin, um die effiziente und kohärente Nutzung des neuen Rechtsrahmens zu maximieren und die Rolle von Europol in Zukunft zu stärken. Insbesondere von Europol gibt es Bedenken, dass die übermäßige Komplexität, Fragmentierung und Länge der Rechtsvorschriften Praktiker oder private Parteien davon abhalten könnte, die neuen verfügbaren Instrumente zu nutzen. Die Bemerkungen der Mitgliedstaaten betreffen vielmehr die Art und Weise, in der Europol Datenschutzgarantien unter der Aufsicht des EDSB restriktiv umsetzt, was die Wirksamkeit und den Mehrwert gewisser Bestimmungen beeinträchtigen könnte.

3.3. Bewertung der Auswirkungen der neuen Befugnisse und Aufgaben von Europol im Bereich der Verarbeitung personenbezogener Daten auf die Grundrechte

Die Kommission fand **keinerlei** Anhaltspunkte für **negative Auswirkungen auf die Grundrechte**, die sich aus der operativen Nutzung der neuen Befugnisse für die Verarbeitung

[42] Verordnung (EU) 2019/818; ABl. L 135 vom 22.5.2019, S. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

personenbezogener Daten ergeben, da die neuen Befugnisse zur Verarbeitung personenbezogener Daten bislang nur begrenzt genutzt wurden.

Neben der Umsetzung der spezifischen Datenschutzanforderungen im Zusammenhang mit den neuen Befugnissen zur Verarbeitung personenbezogener Daten hat Europol schrittweise alle erforderlichen Maßnahmen ergriffen, um die neuen horizontalen Aufsichtsmechanismen in Bezug auf die Grundrechte umzusetzen.

Im Jahr 2024 nahm der Verwaltungsrat von Europol die überarbeiteten Durchführungsbestimmungen des Datenschutzbeauftragten als einen der letzten erforderlichen Durchführungsrechtsakte im Zusammenhang mit der neuen Datenschutzregelung an. Die gesammelten Erkenntnisse deuten darauf hin, dass Europol und ihr Verwaltungsrat in Zusammenarbeit mit dem Datenschutzbeauftragten von Europol und dem EDSB auch für eine **rigorose Umsetzung der** im Jahr 2022 eingeführten **neuen Datenschutzgarantien** gesorgt haben. Dieser Ansatz hat auf den ersten Blick negative Auswirkungen auf die oder Beeinträchtigungen der Rechte des Einzelnen auf Privatsphäre und Schutz personenbezogener Daten durch die anfängliche Nutzung der neuen Befugnisse zur Verarbeitung personenbezogener Daten wirksam verhindert. Den Mitgliedstaaten zufolge verfügt Europol derzeit über einen **soliden Rechtsrahmen für den Datenschutz**, der ausreichende Garantien für eine mögliche verstärkte Nutzung ihrer neuen Befugnisse bietet. Sieben Mitgliedstaaten betonten außerdem, dass dieser Rahmen **den Informationsfluss erleichtert**, indem er das Vertrauen stärkt, auch wenn noch Spielraum für Verbesserungen besteht. Nur ein Mitgliedstaat äußerte einen negativen Standpunkt[43].

Neben den spezifischen **Herausforderungen** im Zusammenhang mit der Kategorisierung betroffener Personen erwähnten Europol und vier Mitgliedstaaten als verbesserungswürdige Bereiche die Kosten und die Zeit im Zusammenhang mit der **Datenschutz-Folgenabschätzung** und der **vorherigen Konsultation** des EDSB, die in der Praxis standardmäßig durchgeführt werden. Eine weitere Herausforderung, die von sechs Mitgliedstaaten angesprochen wurde, ist die Bearbeitung von **Anträgen von betroffenen Personen auf Auskunft** durch Europol, für die es nun auch dann zuständig ist, wenn ein Mitgliedstaat der Dateneigentümer ist.

Der **erste Grundrechtsbeauftragte** wurde im Dezember **2022** ernannt. In den ersten beiden Jahren seiner Amtszeit hat er **keine Beschwerden** erhalten oder beim Exekutivdirektor eingereicht. Der Gemeinsame parlamentarische Kontrollausschuss hat die Tätigkeiten von Europol weiterhin genau überwacht und seit Inkrafttreten der neuen Bestimmungen keine Empfehlungen ausgesprochen. Das Europäische Parlament hat im Februar **2024** das **Konsultationsforum für Grundrechtsfragen des Gemeinsamen parlamentarischen Kontrollausschusses** eingesetzt.

3.4. Kosten-Nutzen-Analyse der neuen Befugnisse und Aufgaben von Europol im Bereich der Verarbeitung personenbezogener Daten

Angesichts des frühen Stadiums der Umsetzung der mit der Verordnung (EU) 2022/991 eingeführten Bestimmungen und der begrenzten Erfahrungen mit ihnen ist es für die Kommission **verfrüht**, aus einer **Kosten-Nutzen-Analyse** aussagekräftige Schlussfolgerungen zu den neuen Bestimmungen zu ziehen.

Die Dienststellen der Kommission haben von Europol Informationen über die bisher im Zusammenhang mit der operativen Durchführung der Verordnung (EU) 2022/991

[43] Siehe Antworten der Mitgliedstaaten auf Frage 9 des kurzen Fragebogens vom 2. Juni 2025 in Anhang III der begleitenden Arbeitsunterlage der Kommissionsdienststellen.

entstandenen Kosten für die zu überprüfenden Bestimmungen eingeholt. Diese Kosten beliefen sich zwischen 2022 und 2025 auf rund **25 Mio. EUR** (etwa 5 % der Gesamtzuweisung an Europol[44]), die in erster Linie einmalige Kosten umfassten. Den Mitgliedstaaten sind bislang keine einschlägigen neuen Kosten im Zusammenhang mit der Verordnung (EU) 2022/991 entstanden.

Die **meisten Kosten** (fast 17 Mio. EUR) betrafen erhebliche Investitionen in die **Entwicklung neuer IKT-Strukturen**, die Umsetzung der Bestimmungen über Forschung und Innovation (das Reallabor ODIN) und in Informationssysteme für den Austausch personenbezogener Daten mit privaten Parteien (PERCI und EU CARES). Auf Kosten für **Personal**, die sowohl für IKT als auch für operative Tätigkeiten anfallen, entfiel etwa ein Drittel der Gesamtausgaben (ca. 8 Mio. EUR). Die Personalkosten werden **auf lange Sicht** die **wichtigsten wiederkehrenden Kosten** darstellen.

Es sei darauf hingewiesen, dass die oben genannten 8 Mio. EUR weder die Personalkosten des für Informationsmanagement zuständigen Referats noch die Ressourcen im Zusammenhang mit (vorherigen und neuen) Aufsichtsmaßnahmen enthalten, die horizontaler Art sind und für die eine Aufschlüsselung auf der Ebene der Umsetzung spezifischer Bestimmungen nicht möglich ist. Die Kosten für diese Mittel sind nicht zu vernachlässigen. So waren im Jahr 2023 schätzungsweise **60 Vollzeitäquivalente (VZÄ)** (fast **5 %** des Europol-Personals) mit Tätigkeiten in **Absicherungs-/Aufsichtsgremien und Aufsichts-/Beratungsstellen** befasst. Europol hat 25 Vollzeitäquivalente für die Reaktion auf die Überwachung des Datenschutzes und die entsprechenden Maßnahmen zur Gewährleistung des Datenschutzes eingesetzt. Dazu gehören Folgemaßnahmen zu den Empfehlungen des EDSB sowie Arbeiten, die im Rahmen früherer Konsultationen zur operativen Datenverarbeitung durchgeführt wurden. Sechzehn dieser 25 VZÄ sind speziell mit Tätigkeiten im Zusammenhang mit den Anforderungen des EDSB befasst. Seit Juni 2025 verfügt Europol über ein spezielles Team von acht Vollzeitmitarbeitern im Bereich des Datenschutzes, einschließlich des Datenschutzbeauftragten.

Europol und fünfzehn Mitgliedstaaten zufolge dürften die **Vorteile** der neuen Befugnisse und Aufgaben im Bereich der Verarbeitung personenbezogener Daten, insbesondere die Analyse großer und komplexer Datensätze sowie die Zusammenarbeit mit privaten Parteien, erheblich sein und **die damit verbundenen Kosten überwiegen**. Kein Mitgliedstaat war anderer Ansicht. Langfristig sind aufgrund von Skaleneffekten und sinkenden Grenzkosten gewisse Effizienzgewinne zu erwarten. Ein Mitgliedstaat betonte, dass es wichtig sei, dass Europol die erforderlichen IKT-Ressourcen bereitstellt, um die Instrumente für die Umsetzung der neuen Möglichkeiten der Verordnung (EU) 2022/991 bereitzustellen und weiterzuentwickeln, was auch von zwei anderen Mitgliedstaaten und anderen Interessenträgern unterstützt wurde[45].

Nach Ansicht von Europol und fünf Mitgliedstaaten müssen mögliche **Ineffizienzen** bei der Umsetzung auch innerhalb des **bestehenden Governance-, Verwaltungs- und Datenschutzrahmens** angegangen werden, um zu vermeiden, dass die operativen Auswirkungen der neuen Aufgaben der Verarbeitung personenbezogener Daten durch eine

---

[44] Im selben Zeitraum beliefen sich die Europol zugewiesenen Haushaltsmittel auf insgesamt etwa **860 Mio. EUR** (die schrittweise von 192 Mio. EUR im Jahr 2022 auf 241 Mio. EUR im Jahr 2025 angestiegen sind). Weitere Einzelheiten finden sich in der begleitenden Arbeitsunterlage der Kommissionsdienststellen.

[45] Siehe die in Abschnitt 5 der diesen Bericht begleitenden Arbeitsunterlage der Kommissionsdienststellen vorgelegten Nachweise, insbesondere die Beiträge von Europol und die Antworten der Mitgliedstaaten auf die Fragen 2, 4 und 5 des kurzen Fragebogens vom 2. Juni 2025 in Anhang III der Arbeitsunterlage der Kommissionsdienststellen und in der Gemeinsamen Erklärung der europäischen Polizeichefs zur Zukunft von Europol.

Verzögerung oder Einschränkung ihrer Nutzung untergraben werden. Fünf Mitgliedstaaten beanstandeten eine zu vorsichtige Umsetzung der Datenschutzbestimmungen durch Europol und ihren Verwaltungsrat unter der Leitung des EDSB. Sie schlagen vor, dass die von den beiden gesetzgebenden Organen eingeräumte Flexibilität angemessen genutzt werden sollte, um die Wirksamkeit und Effizienz der Aufgaben von Europol zu maximieren und ihre Relevanz und langfristige Rentabilität sicherzustellen.

Eine Bewertung der Arbeitsmethoden von Europol und der Bereiche, in denen eine Vereinfachung möglich ist, fällt nicht in den Anwendungsbereich des Berichts nach Artikel 68 Absatz 3 der Europol-Verordnung und wird im Rahmen der Bewertung nach Artikel 68 Absatz 1 der Europol-Verordnung durchgeführt.

4. Schlussfolgerungen und weiteres Vorgehen

Alles in allem kommt die Kommission zu dem vorläufigen Ergebnis, dass die Mitgliedstaaten **weiterhin die Rolle von Europol** in den Schlüsselbereichen **unterstützen**, in denen sie die Mitgliedstaaten derzeit bei ihren **neuen Aufgaben im Bereich der Verarbeitung personenbezogener Daten** unterstützt. Um jedoch die **Vorteile** der neuen Befugnisse zur Verarbeitung personenbezogener Daten zu **maximieren**, müssen nach Ansicht einiger Interessenträger **mögliche Ineffizienzen angegangen werden**, insbesondere innerhalb des bestehenden Governance-, Verwaltungs- und Datenschutzrahmens. Es wäre auch sinnvoll, die **Komplexität und Fragmentierung** des Rechtsrahmens abzumildern, die Praktiker davon abhalten könnten, die neuen Möglichkeiten zu nutzen.

Im Allgemeinen fand die Kommission keine Anhaltspunkte dafür, dass die neuen Vorschriften **negative Auswirkungen auf die Grundrechte** hatten, insbesondere dank solider Datenschutzgarantien, die auch den Informationsfluss erleichtern, indem das Vertrauen der Partner gestärkt wird. Für einige Mitgliedstaaten bevorzugte die Agentur einen konservativen Ansatz, während **die von den beiden gesetzgebenden Organen eingeräumte Flexibilität** in Bezug auf die Kategorisierung betroffener Personen, die Datenschutz-Folgenabschätzung, die vorherige Konsultation des Europol-Datenschutzbeauftragten und die Bearbeitung von Anträgen auf Zugangsrechte angemessen genutzt werden sollte.

Angesichts der allgemein kurzen Umsetzungsfrist der neuen Vorschriften zum Schutz personenbezogener Daten gemäß der Verordnung (EU) 2022/991 sind die gesammelten Erkenntnisse jedoch nicht in allen Fragen schlüssig.

In **ProtectEU**, der Europäischen Strategie für die innere Sicherheit[46], kündigte die Kommission an, dass sie eine ehrgeizige Überarbeitung des Mandats von Europol vorschlagen wird, um die eskalierenden sicherheitspolitischen Herausforderungen anzugehen. Im Einklang mit ihren Leitlinien für eine bessere Rechtsetzung[47] hat die Kommission die Vorbereitungen zur Bewertung der Europol-Verordnung und der Arbeitsmethoden von Europol eingeleitet und den Weg geebnet für einen **Vorschlag der Kommission im Jahr 2026, mit dem die Agentur gemäß den politischen Leitlinien schlagkräftiger gemacht werden soll**[48]. Im Juli 2025 veröffentlichte die Kommission die Aufforderung zur Stellungnahme[49] und beauftragte eine externe Studie zur Unterstützung der Bewertung der Europol-Verordnung und der

[46] ProtectEU – eine Europäische Strategie für die innere Sicherheit, S. 10.

[47] Siehe https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox_de.

[48] Ursula von der Leyen, Politische Leitlinien für die nächste Europäische Kommission 2024-2029, https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_de?filename=Political%20Guidelines%202024-2029_DE.pdf

[49] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14638-Zusammenarbeit-auf-dem-Gebiet-der-Strafverfolgung-neue-Europol-Verordnung-Vorschlag-_de.

Folgenabschätzung für den neuen Vorschlag. Die Bewertung der Europol-Verordnung, die zum Zweck der Erstellung dieses Berichts durchgeführt wurde, soll einen Beitrag zu dieser Bewertung leisten.